CLAIMS

What is claimed is:

1   1.   An authentication method comprising:
2   generating an initialization vector at a first electronic device;
3   determining at the first electronic device whether the initialization vector falls
4   within a first group of initialization vectors, the first group includes a plurality of
5   initialization vectors solely used in connection with an authentication sequence; and
6   encrypting information using in part the initialization vector for return to a
7   second electronic device if the initialization vector falls within the first group.

1   2.   The authentication method of claim 1, wherein the first electronic device
2   is a wireless unit.

1   3.   The authentication method of claim 1, wherein the second electronic
2   device is an access point.

1   4.   The authentication method of claim 1, wherein prior to generating the
2   initialization vector, the method comprises receiving the information from the second
3   electronic device by the first electronic device.

1   5.   The authentication method of claim 4, wherein the information is a
2   challenge text.

1   6.   The authentication method of claim 5, wherein the challenge text is a
2   first sequence of bits and the initialization vector is a second sequence of bits produced
3   by a number generator.

1   7.   The authentication method of claim 4, wherein the number generator is a
2   pseudo-random number generator.

1   8.   The authentication method of claim 1 further comprising regenerating an
2   initialization vector if the initialization vector fails to fall within the first group.

1   9.   The authentication method of claim 1, wherein the determining whether
2   the initialization vector falls within the first group includes determining whether a
3   selected series of bits of the initialization vector has been set.

1   10.   The authentication method of claim 9, wherein the selected series of bits
2   is continuous.

1   11.   The authentication method of claim 5, wherein prior to receiving the
2   challenge text, the method further comprises negotiating a shared secret key between
3   the first electronic device and the second electronic device.

1   12.   The authentication method of claim 11, wherein the encrypting of the
2   information includes
3   combining the initialization vector with the shared secret key; and
4   repeatedly performing bitwise Exclusive-OR (XOR) operations on the challenge
5   text using a combination of the initialization vector with the shared secret key.

1   13.   The authentication method of claim 5 further comprising:
2   transmitting both the encrypted challenge text and the initialization vector to the
3   second electronic device;
4   decrypting the encrypted challenge text using both the initialization vector and a
5   prestored copy of the shared secret key to recover a challenge text; and
6   comparing the recovered challenge text with the challenge text.

1   14.   A method for authenticating a wireless unit in communications with an
2   access point, comprising:
3   transmitting a challenge text from the access point to the wireless unit;
4   receiving an encrypted challenge text and an initialization vector from the
5   wireless unit;
6   decrypting the encrypted challenge text using both the initialization vector and a
7   pre-stored copy of a shared secret key to recover a challenge text; and
8   comparing the recovered challenge text with the challenge text previously
9   transmitted to the wireless unit.

1   15.   The method of claim 14, wherein the challenge text is a first sequence of

2   bits.

1   16.   The method of claim 15, wherein the initialization vector is a second

2   sequence of bits produced by a number generator.

1   17.   The method of claim 16, wherein the number generator is a pseudo-

2   random number generator.

1   18.   The method of claim 14, wherein prior to transmitting the challenge text,

2   the method further comprises negotiating the shared secret key between the access

3   point and the wireless unit.

1   19.   The method of claim 14, wherein the decrypting of the encrypted

2   challenge text includes

3   combining the initialization vector with the shared secret key; and

4   using a combination of the initialization vector and the shared secret key as a

5   key material loaded to decrypt the encrypted challenge text.

1   20.   A method comprising:

2   selecting a bit size (N) of an initialization vector;

3   partitioning all 2^N initialization vectors into a first group and a second group;

4   using an initialization vector from the first group exclusively for authentication;

5   and

6   using an initialization vector from the second group exclusively for data

7   communications.

1   21.   The method of claim 20, wherein the authentication is Wired Equivalent

2   Privacy (WEP) authentication in accordance with Institute of Electrical and Electronics

3   Engineers (IEEE) 802.11.

1   22.   The method of claim 20, wherein a first predetermined number of

2   initialization vectors associated with the first group is substantially less than a second

3   predetermined number of initialization vectors associated with the second group.

1   23.   The method of claim 20, wherein the data communications include
2   wired equivalent privacy (WEP) encryption and WEP decryption operations.

1   24.   An electronic device comprising:
2   a memory to contain a plurality of keys including a shared secret key;
3   a number generator;
4   a device management logic in communication with the memory and the number
5   generator, the device management logic including
6   logic configured to analyze an initialization vector generated from the
7   number generator to determine whether the initialization vector is used for either wired
8   authentication or data communications; and
9   a wireless transceiver to transmit and receive information for configured to
10   support the authentication.

1   25.   The electronic device of claim 24, wherein the authentication is Wired
2   Equivalent Privacy (WEP) authentication.

1   26.   The electronic device of claim 24 is an access point.

1   27.   An electronic device comprising:
2   means for generating an initialization vector;
3   means for determining whether the initialization vector falls within a first group
4   of initialization vectors, the first group includes a plurality of initialization vectors
5   solely used in connection with an authentication sequence; and
6   means for encrypting information using the initialization vector for return to a
7   source for the information using in part the initialization vector if the initialization
8   vector falls within the first group.

1   28.   A software module implemented for execution by an electronic device,
2   the software module comprising:
3   a first module to select a bit size (N) of an initialization vector;
4   a second module to partition all 2^N initialization vectors into a first group and a
5   second group;

6   a third module to use an initialization vector from the first group exclusively for

7   authentication; and

8   a fourth module to use an initialization vector from the second group

9   exclusively for data communications.